wiley

ARTICLE

How Nonprofits Can Protect Against Embezzlement And Fraud

Law360
April 6, 2016

Embezzlement and fraud within nonprofit organizations has reached epidemic proportions. According to an investigation by the Washington Post, between 2008 and 2012 over 1,000 nonprofits reported a "significant diversion of assets" in their IRS Form 990 disclosure forms — in other words, those organizations each suffered losses of over $250,000, or 5 percent of the organization's receipts or assets due to illicit or unauthorized activity.

The vast majority of these nonprofits were public charities, and the top 20 losses alone totaled more than $500 million. And these dismal numbers have not improved since 2012. The 2014 Global Fraud Study by the Association of Certified Fraud Examiners found that on average 5 percent of all nonprofit revenues are lost each year to fraud, with 22 percent of cases involving the loss of more than $1 million. Indeed, just last month, a federal indictment charged Nell Leatherwood, a former Executive Director of the Sequoyah Fund Inc., with a wide-ranging embezzlement scheme involving the use of a corporate credit card and forged checks to steal nearly $1 million from the community development organization, which serves Cherokee communities in North Carolina.

Not surprisingly, the consequences to nonprofit organizations of such illicit activity can be grave. Recovery of funds is often difficult, if not impossible, and can require substantial legal and auditor fees. Indeed, the fraudsters — often employees of the organization — typically use the stolen funds to support a lavish lifestyle such that the funds are no longer available. Moreover, to the extent the theft is covered by an insurance policy, the policy may not reimburse the full amount of the stolen funds. Put simply, if funds are stolen, more often

Authors

Stephen J. Obermeier
Partner
202.719.7465
sobermeier@wiley.law

Practice Areas

Corporate
Employment & Labor
White Collar Defense & Government Investigations

than not, they are gone forever.

Apart from the financial loss directly related to the theft, reputational damage can be even more serious. If the theft — or the organization — is high profile, it may draw unwanted negative media scrutiny that tarnishes the image of the institution in the public eye well into the future. And such reputational damage can lead to dire financial consequences.

Embezzlement can call into question the competence of the organization's staff and may even raise questions regarding the organization's ability to accomplish its stated mission. In such circumstances, an organization may be disqualified from participating in government programs if it has not sufficiently protected government funds. Moreover, private donors, already choosy about the places they give their money, may simply walk away.

As a result, it is imperative that nonprofit organizations be vigilant with respect to protecting against and investigating allegations of embezzlement and fraud. The remainder of this article flags important considerations for nonprofit legal and financial departments and offers some brief guidance on how to protect against fraudulent activity.

What Does Fraud at Nonprofits Look Like?

It is not difficult to imagine how a corporate officer with access to large corporate accounts could defraud an organization out of vast sums of money, and indeed this does happen. For example, on Sept. 17, 2015, a former treasurer of the International Registry of Pathology and executive director of the American Registry of Pathology pled guilty to charges related to his theft of $2.2 million dollars from the organizations. He used organizational accounts that he controlled to transfer money to his personal account and falsified records to make it appear that this money was going towards medical research studies.

But what is surprising is the frequency with which low-level employees have been able to embezzle large amounts of money from nonprofit organizations using relatively simple schemes. For example, one common embezzlement scheme that has resulted in enormous losses to nonprofits involves the submission of phony invoices. An employee submits an invoice on behalf of either a fictitious vendor or a real vendor for services never performed and then intercepts the check and deposits it in a personal bank account. Depending on the invoice amounts, the organization may require only minimal oversight before approving the submission of the invoice or cutting a check, allowing one or two employees to be on both sides of the transaction. And if enough transactions are completed over a long enough time period, they can be difficult to detect and yet result in large losses.

Indeed, this simple scheme was employed with great success by relatively low-level employees in two recent nonprofit fraud cases. One Washington, D.C., organization lost $3.4 million when an information technology employee arranged payments through phony invoices to an IT company for goods that were never provided or for inflated amounts. The fraud went unnoticed because the employee had the ability to both order equipment and log it as having been received. The sophisticated board of the organization, which included two state attorneys general and two governors, failed to recognize the risk in permitting the employee to

operate without oversight or to realize that IT costs for the organization were unusually high.

Similarly, an administrative assistant embezzled more than $5 million from another Washington, D.C., organization by submitting phony invoices for small amounts over the course of several years. The employee created phony invoices on behalf of real vendors or fictitious vendors with similar-sounding names to real vendors, approved them, obtained the resulting checks, and then deposited them into an account she had opened on behalf of the fictitious vendors. Because the vendors on the invoices were either real vendors of the organization or sounded similar to real vendors, for years no one realized that the invoices did not reflect services actually rendered.

In addition to the submission of phony invoices, employees have also defrauded nonprofits through the diversion of funds. In 2011, for example, a former accounting clerk and three other employees of a university were convicted of redirecting $5.7 million in wire transfers that were intended for the university hospital. This type of scheme can also involve the employee endorsing checks made out to the organization and then depositing the funds in his or her own account. An organization is particularly vulnerable to this type of fraud when the organization receives donations that are not specifically expected, as it is not likely to realize the money is missing.

Finally, employees also steal from nonprofits by abusing business expense reimbursement systems. This can be accomplished by paying for personal expenses and submitting the cost to the organization or by submitting reimbursement requests for fictitious or inflated expenses. A former secretary stole $86,000 from a nonprofit organization in Baltimore, in part by misusing the organization's credit card. She also created fake audit reports to cover up her theft.

Why Are Nonprofits Particularly Susceptible to Fraud?

Despite their simplicity, the types of schemes described here are often subtle and can be difficult to detect. But it is also important to recognize that there are many unique features to nonprofit organizations that leave them more susceptible to theft.

First, many nonprofits channel sizeable amounts of funds to others in the form of grants while still operating with minimal staff. At these types of institutions, significant losses may go unnoticed because of the sheer volume of funds that are being managed by relatively few people.

Additionally, at many nonprofit organizations, accounting and compliance staff is considered "overhead" that does not directly contribute to the organization's mission. As a result, it is not uncommon for nonprofit organizations to face pressure to cut such overhead. This can leave an organization without sufficient resources to properly manage the flow of funds.

Finally, and perhaps most importantly, the culture of nonprofit organizations often makes detecting fraud more difficult. As organizations with a charitable mission, they tend to attract employees with a humanitarian outlook, and managers often assume that their employees are working there to promote a common, charitable vision. A sense of camaraderie and mutual reliance is common. In that kind of atmosphere, the

possibility of illegal theft may seem implausible, and genuine trust may lead managers to overlook the need to have robust compliance programs to scrutinize financial transactions and employee behavior — especially with respect to low-level employees and small financial transactions — as would be typical at a for-profit firm.

What Can Be Done to Prevent Fraud at Nonprofits?

One might expect that regular external financial audits can be counted on to detect theft, but this is in fact rarely true. Traditional financial audits, whether in the nonprofit or for-profit sectors, are not designed to ferret out fraud. For example, examining a sample of transactions may miss even a substantial amount of fraudulent activity, and when an insider is stealing, they may possess enough knowledge to fool auditors with backup documentation that appears authentic. In those cases, a normal balancing of the books will allow the fraud to remain hidden.

Indeed, the organization victimized by the phony invoice scheme described above had been conducting regular external financial audits and still failed to uncover the substantial fraud until irregular activity was detected by one of the organization's financial institutions. The Association of Certified Fraud Examiners reports that external audits detected only 3 percent of the frauds reported to it and includes among its recommendations that "external audits should not be relied upon as an organization's primary fraud detection method."

As a result, by far the most effective way to deal with embezzlement is to prevent it before it begins through rigorous internal controls. Again, a regular external program audit not specifically focused on internal fraud detection cannot necessarily be counted on to reveal weaknesses in the organization's controls. Rather, outside review by experienced counsel or consultants specifically employed to evaluate internal controls should be employed. From this assessment, an organization can work towards implementing appropriate protections.

Although the nature of an organization's fraud protection program will be specific to that organization, there are best-practices that should be utilized by any organization wishing to implement such an apparatus.

First, board members and executive-level employees must set the right tone. The board and organization executives must communicate, both explicitly and implicitly, that behavior inconsistent with the mission of the organization will not be tolerated. In financial matters, the board is responsible for setting an attitude of compliance and respect for procedure. The board, executives and other organization leaders need to make it clear that financial controls and procedures are not obstacles or irrelevant paperwork; rather, they are an important component of making sure the organization stays focused on its goals.

Second, the organization must advocate strongly with its donors that adequate funding to implement basic financial controls, including funding for associated staff time, is essential to safeguarding the donor's contribution. It is important for donors to understand that they can play a role, inadvertently, in the proliferation of fraud and abuse if they require large donations to be used without minimum necessary administrative support for financial controls.

Third, board members and executive-level employees must properly exercise oversight of the organization. Major transactions should be subject to board approval, and the board should also conduct regular reviews of the financial data of the organization and assessments of financial controls. Nonprofit boards often contain influential people in the area that the organization operates but who do not have substantial managerial or oversight experience. Nevertheless, every board member should understand that it is their job to ensure that the organization has adequate anti-fraud policies and procedures. If possible, the board should establish a separate finance committee consisting of individuals experienced in finance and accounting. A finance committee should make sure that all data presented to the board is verified and should review budgets closely to ensure that they are reasonable in light of past actual expenses of the related program.

Fourth, nonprofits should develop policies that create a culture of compliance and ensure that all employees are aware of the possibility of fraud. A code of ethics should be created that includes fraud policies and how to respond to hints of wrongdoing. A hotline should be established so that anonymous tips can be made, even if it is only a separate mailing address for board members overseeing finances. Indeed, the 2014 Global Fraud Study found that tips are by far the most common method of detection, and organizations with hotlines detected frauds more quickly and the frauds were less costly.

Fifth, it is important to shape operational procedures regarding disbursements and the receipt of funds with compliance controls in mind. Of course, these procedures must be scaled to the size of the organization, but any size organization can utilize financial controls. There should be as much diversification of authority and roles of employees as possible so that financial transactions are reviewed by more than one party.

For example, if an executive has an organization credit card that is used to pay for business expenses, someone else should review the charges to ensure that it is not being used for personal expenses. It is also advisable that monthly statements be sent directly to the board by those preparing them so that the status of financial accounts can be assessed apart from what organizational leaders may be reporting. An organization should develop a close working relationship with the bank it uses, and restrictive endorsements should be used on all checks above reasonable thresholds. If an organization deals with donated goods and services, they need to be controlled and tracked just like the inventory of a business.

Sixth, organizations should conduct a regular review of their insurance policies so that if a fraud does occur, the organization and its directors and officers are adequately protected.

Most importantly, organizations and donors need to take the threat of fraud and embezzlement seriously. Fraud is a real danger for every organization, and proactive steps must be taken to minimize its risk. In the words of Dr. Cheryl Healton, the former president and CEO of the defrauded American Legacy Foundation, "I would caution organizations on the need for rigorous internal and external controls, because fraud can happen even in an atmosphere of best intentions. No matter how much you value your employees, trust cannot be an internal control."